REMARKS

The last Office Action in the above-identified application and the reference cited by the Examiner have been carefully considered. For the reasons stated below, it is respectfully urged that Claim 2, the only claim in this case, patentably distinguishes over the reference cited and is allowable in its present form.

This application is a continuation of Applicants' previous application Serial No. 09/154,133, which has now matured into U.S. Patent No. 6,307,936. Examiner Todd Jack was the Examiner for the previous application.

Claim 2 of this application is exactly the same as Claim 1 of U.S. Patent 6,307,936, except that the fifth method of generating a key set forth in Claim 1 of the '936 patent has been changed in this continuation application.

In the '936 patent, the method of managing encryption keys in a cryptographic co-processor has as its third listed step "generating a key", and one of the ways of generating the key was listed as transforming a key using at least one of hashing, mixing with fixed data and re-hashing, and exclusive oring (XORing). This was the fifth way of six possible ways of generating the key which is set forth in Claim 1 of the '936 patent.

In Claim 2 of the subject continuation application, which is the only claim in the case, the claim is exactly the same as Claim 1 of the '936 patent except that the fifth way of generating a key is defined as "transforming an existing key". All of the other five ways of generating the key, and all of the other limitations in Claim 2, are exactly the same as they are recited in Claim 1 of the '936 patent.

For the Examiner's convenience, a copy of a Supplemental Amendment filed on March 19, 2001 in the parent '936 patent, in which amendments to Claim 1 were courteously suggested to be made by Examiner Jack during a telephone conference on March 8, 2001, to overcome the citation of the Barkan patent, is submitted herewith.

Also for the Examiner's convenience, Applicants wish to repeat below the Examiner's statement of reasons for allowance of essentially the same claim (Claim 1) of the '936 parent application:

> The applicant, on a response to the examiner's 1st action, has amended the one claim of the case to overcome the examiner's rejection. The applicant teaches 1) that the user selects the key, 2) the key management method supporting three types of key encryption keys (KEKs), and the symmetrical key generation can preferably be performed in six ways. The examiner has been unable to find the particulars of the above teachings in the prior-art searched.

First, Applicants respectfully believe that Claim 2 of the subject continuation application should have been rejected on obviousness-type double patenting grounds in view of Claim 1 of the '936 patent, as Claim 2 of the subject continuation application is essentially the same as Claim 1 of the '936 patent except for the minor change in the fifth out of the sixth ways of generating the key. Applicants offer to submit a Terminal Disclaimer if Examiner Jack instructs Applicants to do so. In this regard, it would be appreciated if Examiner Jack would contact the undersigned attorney at the telephone number given below if he would like Applicants to file such a Terminal Disclaimer, and Applicants would be more than willing to follow the Examiner's request in this regard.

Second, it is respectfully urged that Claim 2 patentably distinguishes over the Barkan (U.S. Patent No. 5,864,667) for the same reasons submitted with respect to Claim 1 of the '936 patent, as the two claims are essentially the same except for a minor change in the fifth out of six ways of generating the key, which is the third listed step in Applicant's method of managing encryption keys in a cryptographic co-processor.

Specific comments comparing the Barkan patent to the method set in Claim 2 are respectfully provided below for the Examiner's consideration.

The Barkan patent is directed to a method and apparatus for distributing encryption keys to establish a secure link between computer users at different locations without prior secure communication between the parties. In a first embodiment of the invention, a key

management device attached to the user's encryption machine contains a list of secure communication partners and their respective encryption keys. To initiate a secure link session, the user identifies the desired addressee, and the encryption key and other parameters corresponding to the desired addressee are automatically transferred to the encryption machine.

In a second embodiment of the invention described in the Barkan patent, if the desired addressee is not found in the key management device, the encryption key and parameters corresponding to the desired addressee are obtained from a key distribution center. This information is then transferred to the encryption machine and stored in the key management device.

In a third embodiment, communication with the key distribution center is encrypted using a public/private key algorithm to prevent eavesdropping. In a fourth embodiment of the invention, a user's key distribution device acts as an intermediary between the key distribution center and the user. In a fifth embodiment, a wide area network of key distribution devices is provided for rapidly updating key distribution information. Additional embodiments of the invention concern various applications of a certificate or digital safe key/identification package.

However, the Barkan patent does not disclose a method of managing the use of keys, which includes selecting a key, selecting a bit length for the key, generating the key, and representing the key in one of an external form and an internal form within a cryptographic coprocessor, as defined by Claim 2. In addition, the quantity of encryption key algorithms, which are supported by the method and apparatus disclosed in the Barkan patent, appears to be limited.

The Barkan patent was distinguished over in the earlier '936 patent, which is the parent of the continuation application now under examination. The Examiner agreed that no reference teaches 1) that the user selects the key, 2) the key management method supporting three types of key encryption keys (KEKs), and 3) the symmetrical key generation can preferably be performed in six ways.

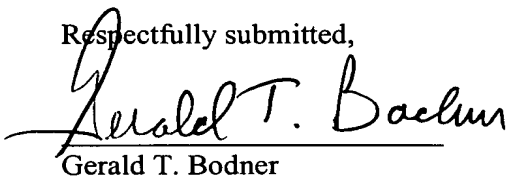
In Claim 2 of the continuation application, there are still six ways defining the symmetrical key generation. The difference between the claim in the earlier patent and the pending claim in this continuation application is the fifth listed way of generating a key. In the earlier patent, one of the ways of generating the key was listed as transforming a key using at least one of hashing, mixing with fixed data and re-hashing, and exclusive oring (XORing). In the claim now on file, Applicants instead recite that one of the six ways of generating a key is by transforming an existing key.

It is respectfully urged that the Barkan patent does not show any of the specific limitations set forth in the claim, including the fifth out of six enumerated ways of generating the key, that is, by transforming an existing key, in conjunction with all of the other steps and limitations set forth in Claim 2. Accordingly, it is respectfully urged that Claim 2 patentably distinguishes over the Barkan patent and is allowable.

Applicants appreciate the Examiner's suggestions in the parent '936 patent for overcoming the Barkan patent and, in this continuation application, Applicants would appreciate the Examiner's consideration of the statements made herein in support of the patentability of Claim 2, the only claim set forth in this continuation application. In order to expedite the prosecution of this application, if Examiner Jack would prefer to telephone the undersigned attorney at the telephone number given below to advise him whether a Terminal Disclaimer should be filed, this would be much appreciated and the undersigned attorney will immediately file such a Terminal Disclaimer for the Examiner's consideration.

In view of the foregoing remarks, reconsideration of Claim 2 and allowance of this continuation application with Claim 2 are respectfully solicited.

Respectfully submitted,



Gerald T. Bodner
Attorney for Applicant
Registration No. 30,449

BODNER & O'ROURKE, LLP
425 Broadhollow Road, Suite 108
Melville, New York 11747
Telephone: (631) 249-7500